Bernd Zwattendorfer, Bojan Suzic, Peter Teufl, Andreas Derler - "Sicheres Speichern in der Public Cloud mittels Smart Cards" - D-A-CH Security 2013, pp. 120-132

Sicheres Speichern in der Public Cloud mittels Smart Cards

Bernd Zwattendorfer[1], Bojan Suzic[2], Peter Teufl[2], Andreas Derler[3]

[1]E-Government Innovationszentrum (EGIZ)
bernd.zwattendorfer@egiz.gv.at

[2]A-SIT - Zentrum für sichere Informationstechnologie - Austria
{bojan.suzic, peter.teufl}@a-sit.at

[3]Technische Universität Graz
andreas.derler@student.tugraz.at

Zusammenfassung

Das Speichern von Daten in der Public Cloud bringt viele bekannte Probleme im Zusammenhang mit dem Datenschutz und der Sicherheit dieser Daten. Eine mögliche Lösung für diese Probleme ist das Verschlüsseln der Daten am Client – z.B. Smartphone, Tablet, Desktop, oder Browser – bevor diese beim jeweiligen Cloud-Provider abgelegt werden. Obwohl diese Lösung nicht für alle Anwendungsszenarien verwendet werden kann, stellt sie gerade für Online-Speicher (z.B. DropBox, Google Drive, SkyDrive) eine interessante und vor allem in Bezug auf die Sicherheit wirksame Lösung dar. Es existieren bereits zahlreiche Lösungen, die die Daten vor dem Ablegen bei diesen Cloud-Providern am Client verschlüsseln bzw. nach dem Abrufen wieder entschlüsseln. Allerdings bringen diese Lösungen auch Probleme mit sich, die vor allem das Schlüsselmanagement und das Verteilen verschlüsselter Daten an mehrere Benutzer betreffen. Aus diesem Grund wird in der folgenden Arbeit eine Software vorgestellt, die diese Probleme beim sicheren Ablegen von Daten auf gängigen Cloud-Storage Lösungen umgeht. Die Probleme des Schlüsselmanagements und der sicheren Aufbewahrung dieser Schlüssel werden dabei mit Hilfe der von der österreichischen Bürgerkarte aufgebauten Public Key Infrastructure (PKI) umgangen. Die vorgestellte Software verwendet dabei das S/MIME Format um sichere Container zu erstellen, die dann mit anderen Benutzern geteilt werden können. Aufgrund der bereits vorhandenen PKI, erfolgt der Schlüsselaustausch der öffentlichen Schlüssel über vertrauenswürdige X509-Zertifikate. Die Sicherheit der privaten Schlüssel und deren Aufbewahrung ist dabei aufgrund der Speicherung auf einer Smart Card (der österreichischen Bürgerkarte) gewährleistet.

1 Einleitung

Cloud Computing und Cloud Dienste werden derzeit sehr häufig zum Speichern von Daten auf externen Systemen verwendet, z.B. zu Archivierung oder Backup-Zwecken. Populäre Beispiele dafür sind beispielsweise DropBox oder Google Drive. Diese Cloud Dienste erlauben das Speichern und die Dateien-Synchronisation in der Cloud unter Verwendung unterschiedlicher Clients.

Während einfache Daten problemlos in der Cloud abgelegt werden können, so sind bestimmte Sicherheitsaspekte zu beachten, wenn sensible Daten in der Cloud gespeichert werden sollen. Üblicherweise sind sensible Daten aufgrund von Richtlinien oder Gesetzen speziell zu schützen und vor unautorisierten Zugriff zu bewahren. Im Fall von den meisten Cloud Diensten sind diese Anforderungen nicht so einfach zu erfüllen, da der Cloud Provider immer Einsicht auf die Daten nehmen könnte, sofern diese nicht verschlüsselt abgelegt sind und der Provider auch nicht den dazugehörigen Schlüssel besitzt.

Um sensible Daten dennoch in der Cloud sicher ablegen zu können, bieten einige Cloud-Anbieter bereits Lösungen an, bei denen die Daten vor dem Transfer client-seitig verschlüsselt werden. Einige solcher Anbieter werden im folgenden Abschnitt 2 kurz vorgestellt. Alle diese Anbieter haben jedoch den Nachteil, dass die Schlüsselpaare zum Ver- und Entschlüsseln der Daten nur softwaremäßig am jeweiligen Client gespeichert sind. In diesem Artikel stellen wir jedoch eine Lösung vor, die zum sicheren Speichern von Daten in der Public Schlüsselpaare verwendet, die hardware-mäßig in einer Smart Card integriert sind. Als Beispiel für eine Smart Card wird die österreichische Bürgerkarte verwendet, hinter der auch eine komplette PKI-Infrastruktur steht. Somit ist es theoretisch möglich, Daten für jeden beliebigen österreichischen Bürger zu verschlüsseln und in einer Public Cloud abzulegen. Im Rahmen dieses Artikels wird die Implementierung und Umsetzung dieser Lösung vorgestellt und deren Vor- und Nachteile gegenüber bereits existierenden Lösungen evaluiert.

2 Related Work

Der Wunsch Daten sicher zu speichern und vor unerlaubten Zugriff zu schützen ist nicht neu. Viele Ansätze existieren bereits, um Daten sicher und vertraulich auf lokalen oder entfernten Systemen abzulegen. Üblicherweise werden für die Anforderung des vertraulichen Speicherns von Daten unterschiedliche Verschlüsselungstechniken eingesetzt. In diesem Abschnitt werden deshalb unterschiedliche Ansätze beschrieben, die Verschlüsselungstechniken verwenden, um Daten sicher und vertraulich auf entfernten Systemen, wie es z.B. die Public Cloud darstellt, abzulegen.

Aktuell befassen sich die gängigsten Ansätze für die Sicherstellung des Schutzes der Vertraulichkeit von Daten mit Container-Formaten, die die zu schützenden Daten in einem Container verpacken, welcher einfach verschlüsselt werden kann. Ein populäres Beispiel für so ein Container-Format ist der S/MIME (Secure/Multipurpose Internet Mail Extensions) Standard [RT04], welcher häufig für das Verschlüsseln und das sicher und vertrauliche Versenden von E-Mails eingesetzt wird. Ein anderes populäres und weit-verbreitetes Beispiel für eine Software zum Verschlüsseln von Daten ist TrueCrypt[1]. Neben der Möglichkeit der Verschlüsselung von Containern ist es mit Hilfe von TrueCrypt möglich, auch ganze Partitionen oder Festplatten zu verschlüsseln. Nachdem dieser Container-Ansatz zur sicheren Datenspeicherung nicht neu ist, existiert auch eine Reihe anderer Software, die die Verschlüsselung von Containern im lokalen System unterstützt.

Speziell die steigende Popularität von Cloud Computing hat dazu geführt, dass neue Lösungen für ein sicheres und vertrauliches Speichern von Daten in entfernten Systemen entwickelt wurden. Das vertrauliche und sichere Speichern von Daten in der Cloud ist besonders essentiell, wenn es sich um sensible oder persönliche Daten handelt [EP95]. Im Wesentlichen soll

[1] http://www.truecrypt.org

dabei vermieden werden, dass der Cloud Provider, welcher die Daten speichert, unbefugten Zugriff auf die Daten und deren Inhalt bekommt. Nachdem sich Cloud Computing in den letzten Jahren sehr stark entwickelt hat, existieren auch hier bereits einige Ansätze, um Daten sicher und vertraulich in der Cloud zu speichern. Ein Beispiel ist der sogenannte Middleware-Ansatz, bei dem die in der Cloud zu speichernden Daten zuerst von einer Middleware verschlüsselt werden, bevor die Daten tatsächlich in der Cloud abgelegt werden. Der erwähnte Middleware-Ansatz wird beispielsweise in [DHC+12] oder [SGS11] beschrieben. Aber auch der bekannte und populäre Cloud-Speicherdienst DropBox[2] setzt auf gewisse Art und Weise auf diesen Middleware-Ansatz. DropBox verwendet nämlich die Services und Server von Amazon S3[3] zum Speichern der Daten, jedoch verschlüsselt DropBox die Daten, bevor sie zu den Amazon Servern transferiert werden [DropBox]. Obwohl die Daten hier verschlüsselt bei Amazon liegen, hat dieser Ansatz den Nachteil, dass die Verschlüsselungs-Schlüssel dennoch von der Middleware, und somit in diesem Fall von DropBox, verwaltet werden. Die Middleware hat somit immer die Möglichkeit, die Daten auch im Klartext zu beziehen.

Ausgereiftere und fortgeschrittene Software für das sichere und vertraulichere Speichern in der Cloud setzen auf einen benutzer-zentrierten Ansatz, welche Verschlüsselungstechniken nicht bei einer Middleware, sondern bereits auf Client-Seite einsetzen. In diesem Fall werden die Daten bereits auf Client-Seite beim Benutzer verschlüsselt, bevor die Daten in die Cloud übertragen werden. Der Vorteil bei diesem Ansatz ist, dass die Verschlüsselungs-Schlüssel immer im Besitz des Benutzers bleiben und der Cloud Provider, bei dem die Daten abgelegt werden, keine Möglichkeit besitzt, die gespeicherten Daten zu entschlüsseln. Implementierungen dieses Ansatzes sind beispielsweise die Services Wuala[4], BoxCryptor[5] oder SpiderOak[6]. Nichtsdestotrotz besitzen dieses Services den Nachteil, dass nur Software-Schlüssel zum Einsatz kommen.

Um diesen Nachteil entgegen zu wirken, wird in weiterer Folge ein Ansatz vorgestellt, der zwar ebenfalls benutzer-zentriert ist, jedoch hardware-basierte Schlüssel, welche auf Smart Cards hinterlegt sind, zum sicheren und vertraulichen Speichern von Daten in der Cloud zum Einsatz bringt.

3 Citizen Card Encrypted (CCE)

Die folgenden beiden Unterkapitel beschreiben kurz das Konzept der österreichischen Bürgerkarte sowie eine Software, die die Bürgerkarte zum sicheren Ver- und Entschlüsseln von Daten verwendet.

3.1 Das Konzept „Bürgerkarte“

Die österreichische Bürgerkarte [LHP02] [HKR+08] ist eine Kernkomponente und ein wesentlicher Bestandteil im österreichischen E-Government. Sie dient vor allem dazu, die Kommunikation in elektronischen behördlichen Verfahren zwischen Bürgern und Behörden zu vereinfachen, zu beschleunigen, und sicher zu gestalten. Im Prinzip stellt die österreichi-

[2] https://www.dropbox.com

[3] http://aws.amazon.com/s3

[4] http://www.wuala.com

[5] https://www.boxcryptor.com

[6] https://spideroak.com

sche Bürgerkarte einen digitalen amtlichen Ausweis im Internet für österreichische Bürger dar.

Im Allgemeinen wird der Begriff „Bürgerkarte“ eher als Konzept betrachtet, da das österreichische E-Government-Gesetz [EGovG], in dem die Bürgerkarte definiert ist, speziell die Technologieneutralität und die Unabhängigkeit von technischen Komponenten hervorhebt. Aufgrund dieser festgeschriebenen Technologieneutralität kann es zu unterschiedlichen Ausprägungen und Implementierungen einer Bürgerkarte kommen. Die derzeit häufigste Ausprägung der österreichischen Bürgerkarte ist eine Smart Card, wie sie z.B. Bankomatkarten oder Gesundheitskarten darstellen. Jeder österreichische Bürger ist beispielsweise mit einer Gesundheitskarte der österreichischen Sozialversicherung (*e-card*) ausgestattet, bei der einfach und nach Wunsch jederzeit die vorinstallierte Bürgerkartenfunktionalität aktiviert werden kann. Nichtsdestotrotz existieren auch andere Ausprägungen der Bürgerkarte, wie z.B. die sogenannte Handy-Signatur[7], welche auf der Verwendung eines Mobiltelefons und einem server-seitigen Hardware-Sicherheitsmodul (HSM) basiert.

Die wesentlichen Funktionen der österreichischen Bürgerkarte sind im E-Government-Gesetz geregelt. Dies sind vor allem:

- Die Identifizierung und Authentifizierung eines Bürgers
- Die Erstellung qualifizierter elektronischer Signaturen
- Die Verschlüsselung von Daten

Mit Hilfe der Bürgerkarte können österreichische Bürger bei Online Applikationen sowohl des behördlichen als auch des privatwirtschaftlichen Bereichs sicher und eindeutig identifiziert und authentifiziert werden. Die Bürgerkarte enthält auch ein qualifiziertes Zertifikat gemäß der EU-Signaturrichtlinie [SigR], wodurch elektronische Signaturen, welche mit einer Bürgerkarte erstellt worden sind, einer handschriftlichen Unterschrift gleichzustellen sind. Neben dem Signaturzertifikat ist auch ein weiteres Schlüsselpaar gespeichert, welches zum sicheren Ver- und Entschlüsseln von Daten verwendet werden kann. Die öffentlichen Verschlüsselungsschlüssel eines einzelnen Bürgers sind dabei über ein zentrales LDAP[8]-Verzeichnis abrufbar. Somit können für jeden österreichischen Bürger bei Bedarf Daten verschlüsselt und somit vertraulich abgelegt werden. Im weiteren Teil dieser Arbeit betrachten wir nur mehr diese Ver- und Entschlüsselungsfunktion der österreichischen Bürgerkarte.

3.2 Die Software CCE

Die CCE[9] (Citizen Card Encrypted) Software ist ein plattformunabhängiges, von A-SIT[10] (Zentrum für sichere Informationstechnologie – Austria) entwickeltes Open Source-Tool, das die Umsetzung von besonderen Bedürfnissen von österreichischen Behörden und staatlichen Einrichtungen in Hinsicht Datensicherheit- und -verwaltung unterstützt. Es ermöglicht das Verschlüsseln, Entschlüsseln und allgemein das Management von Daten und Verzeichnissen, sowohl für Einzelpersonen als auch für Personengruppen.

[7] http://www.handy-signatur.at

[8] Lightweight Directory Access Protocol

[9] http://demo.a-sit.at/buergerkarte/cce/index.html

[10] http://www.a-sit.at

Für die Verschlüsselung und Entschlüsselung von Dateien oder Verzeichnissen können mittels CCE entweder die österreichische Bürgerkarte, bei der die entsprechenden Schlüssel hardwaremäßig gespeichert sind, oder Software-Schlüssel eingesetzt werden. Die Anwendung von der Bürgerkarte ermöglicht besonders den sicheren Datenaustausch und die sichere Datenaufbewahrung, da die notwendigen Schlüssel hardwaremäßig gespeichert sind und nicht von einer Anwendung ausgelesen werden können. Das CCE-Tool unterstützt dabei die Bürgerkarte nur in Ausprägung einer Smart Card, da derzeit von der server-seitigen Handy-Signatur keine Ver- und Entschlüsselungsfunktionalität bereitgestellt wird. Durch den modularen Aufbau von CCE können jedoch auch weitere Smart Card-Implementierungen einfach integriert werden. Somit können auch andere PKI-Lösungen unterstützt werden.

CCE verwendet S/MIME [RT04] als Container-Format zum sicheren Abspeichern von Daten, welches breit anerkannt und auch in gängigen E-Mail-Clients zum Verschlüsseln von E-Mails Verwendung findet. Im Folgenden werden die wichtigsten Eigenschaften und Features von CCE mit Relevanz für diese Arbeit ausgewiesen:

Smart Card – Sichere Entschlüsselungseinheit

Die Operationen zum Entschlüsseln von Daten werden direkt auf der Karte durchgeführt, wobei der Besitzer der Karte einen entsprechenden PIN eingeben muss, um den Vorgang auszulösen. Da das Verschlüsselungsverfahren von der Bürgerkarte asymmetrische Schlüssel verwendet und somit höhere Rechenleistung benötigt, werden die Daten im Fall von CCE zuerst mit einem symmetrischen Schlüssel am Rechner des Benutzers verschlüsselt. Anschließend wird das asymmetrische Verschlüsselungsverfahren von der Karte angewandt und der verwendete symmetrische Schlüssel damit verschlüsselt. Dieser Schlüssel wird dann gemeinsam mit den verschlüsselten Daten im CCE-Container integriert und abgespeichert.

Unterstützung von Gruppenverschlüsselung

Dateien und Verzeichnisse können mittels CCE für mehrere Benutzer verschlüsselt werden, die durch eine Gruppe oder Untergruppe definiert sind. Die Definition und Verwaltung von Gruppen wird üblicherweise vom Benutzer selbst oder organisationsweit durchgeführt. Die Gruppenverschlüsselung erlaubt somit auch den Einsatz von Backup-Schlüsseln.

Unterstützung österreichischer PKI Infrastruktur

Das asymmetrische Verschlüsselungsverfahren erleichtert die Verschlüsselung von Daten für bestimmte Personen oder Gruppen. Die öffentlichen Schlüssel von den Empfängern sind dabei über die österreichische PKI-Infrastruktur öffentlich verfügbar und über den öffentlichen LDAP-Abfragepunkt abgreifbar. Der interne Aufbau von CCE erlaubt jedoch auch die Integration einer beliebigen PKI-Infrastruktur (z.B. aus dem Unternehmensbereich).

Sicheres Löschen von Dateiresten

Üblicherweise werden die zu ent- oder verschlüsselnden Dateien im Prozess temporär gespeichert, sodass möglicherweise über diese temporären Dateien Rückschlüsse auf die eigentlichen Original-Dateien gemacht werden können. CCE unterbindet solch mögliche Rückschlüsse, indem diese Dateien sicher und rückschlussfrei gelöscht werden.

4 Architektur und Vergleich

In diesem Abschnitt wird die Architektur unserer Smart Card-basierten Lösung zum sicheren und vertraulichen Speichern von Daten in einer Public Cloud genauer beschrieben. Daneben wird der Verschlüsselungsvorgang näher erläutert. Im zweiten Unterabschnitt wird unsere Lösung anschließend gegen andere Ansätze verglichen und abgegrenzt.

4.1 Architektur und Funktionsweise

Funktionell wurde die Software CCE dabei dahingehend erweitert, sodass verschlüsselte Daten nicht nur lokal, sondern auch bei ausgewählten Public Cloud Providern abgelegt werden können. Bürger können dabei den Cloud Anbieter, bei dem die Daten abgelegt werden sollen, selbst wählen. In der derzeitigen Umsetzung werden die beiden Public Cloud Anbieter *DropBox*[11] und *Google Drive*[12] unterstützt.

Abbildung 1 zeigt im Wesentlichen die Architektur zum sicheren und vertraulichen Speichern von Daten in der Public Cloud unter Verwendung der Ver- und Entschlüsselungsfunktionen der österreichischen Bürgerkarte.

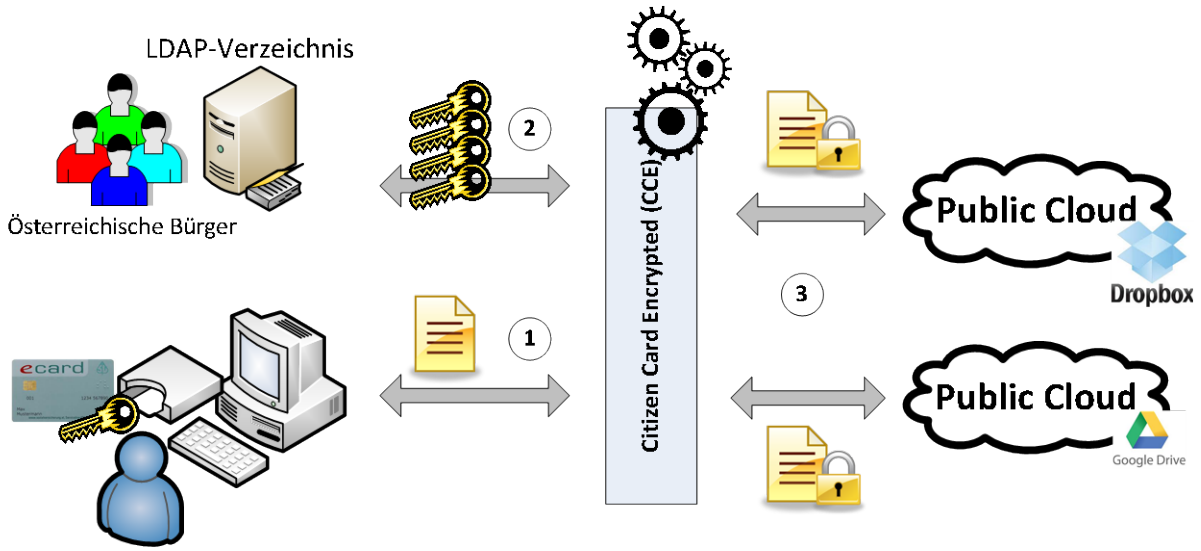

Abbildung 1 - Architektur der Smart Card-basierten Lösung zum sicheren und vertraulichen Speichern in der Public Cloud

Abbildung 1 illustriert auch beispielhaft einen Verschlüsselungsvorgang mittels CCE und anschließendem sicheren Speichern in der Public Cloud. Dabei wählt der Bürger in einem ersten Schritt (Schritt 1) jene Dateien oder Verzeichnisse aus, welcher er sicher und vertraulich in der Public Cloud ablegen möchte.

In einem nächsten Schritt (Schritt 2) selektiert der Bürger dann jene Personen (österreichische Bürger) oder Gruppen, für welche die Daten verschlüsselt werden sollen. Die Empfänger werden in der Regel im persönlichen oder organisatorischen Empfängerverzeichnis eingetragen und notwendigerweise in Gruppen unterteilt. Nicht eingetragene Empfänger werden ein-

[11] https://www.dropbox.com

[12] https://drive.google.com

fach per Abfrage an das in Abschnitt 3.1 erwähnte zentrale LDAP-Verzeichnis gesucht, in welchem die Verschlüsselungszertifikate aller österreichischen Bürger gelistet sind. Vor dem Verschlüsselungsvorgang werden die Zertifikate der Empfänger noch auf ihre Gültigkeit überprüft.

Im abschließenden Schritt 3 werden die Daten mit Hilfe von CCE für die ausgewählten Bürger verschlüsselt und sicher zum ausgewählten Public Cloud Provider übertragen. Die Credentials (Benutzername/Passwort) für einen authentifizierten Zugang zur Public Cloud müssen nur bei der Konfiguration des Cloud Providers in CCE eingegeben werden. Eine Authentifizierung am Public Cloud Provider für einen Datei-Upload erfolgt danach automatisch.

Ein Entschlüsselungsvorgang erfolgt ähnlich und ist daher nicht mehr bildlich dargestellt. Die verschlüsselten Dateien oder Verzeichnisse werden dabei in einem ersten Schritt vom Benutzer von der Public Cloud in das lokale System heruntergeladen. Anschließend werden die Daten mit Hilfe von CCE und der Smart Card des Benutzers entschlüsselt und stehen zur weiteren Verwendung und Einsicht zur Verfügung. Details zur Umsetzung von Ver- und Entschlüsselung von Daten mittels Bürgerkarte und dem sicheren Speichern in der Public Cloud werden in Abschnitt 5 genauer beschrieben.

4.2 Vergleich mit anderen Lösungen

Im Abschnitt 2 wurden andere Ansätze und Lösungen für ein sicheres und vertrauliches Speichern in der Cloud vorgestellt. In diesem Unterabschnitt wird unsere präsentierte Lösung mit diesen existierenden Lösungen verglichen und Vor- und Nachteile erarbeitet.

4.2.1 Vorteile

Dieser Abschnitt beschreibt die Vorteile unserer Lösung gegenüber den in Abschnitt 2 genannten Diensten.

Verwendung externer PKI-Infrastruktur

Alle in Abschnitt 2 genannten Dienste basieren auf einem eigenen Verschlüsselungssystem. Um bei der Ver- und Entschlüsselung und dem Austausch von Daten teilnehmen zu können, müssen alle teilnehmenden Benutzer bei demselben Cloud Dienst registriert sein. Hier spricht für CCE, dass die Software mit einer externen PKI Infrastruktur kompatibel ist, die von öffentlichen Einrichtungen begründet wurde und die allen Bürgern frei zur Verfügung steht. Sobald ihre Bürgerkarte aktiviert ist, brauchen weder Versender noch Empfänger irgendwelche zusätzlichen Registrierungsprozesse. Sie können Daten für andere Bürger einfach und mühelos verschlüsseln, ohne speziell Kontakt miteinander aufnehmen zu müssen, um Schlüssel oder Passworte auszutauschen. Im Allgemeinen ist CCE so aufgebaut, dass nicht nur die PKI-Infrastruktur der öffentlichen Verwaltung für Bürger verwendet werden muss, sondern jede beliebige Infrastruktur, z.B. eines Unternehmens, welches intern Smart Cards verwendet, einfach integriert werden kann.

Kein Vendor Lock-In

Die für die Verschlüsselung verwendeten Schlüssel werden nicht von CCE, sondern von einer externen Institution verwaltet. Das hat zur Folge, dass CCE neutral und vom Cloud Anbieter unabhängig ist. Benutzer können den Cloud-Anbieter einfach wechseln, ohne dass interne Organisationsprozesse angepasst werden müssen.

Sichere, hardware-basierte Entschlüsselung

Im Fall von CCE wird für die Entschlüsselung von Daten ein sicheres, hardware-basiertes Gerät verwendet. Damit wird die Sicherheit gegenüber anderen Cloud-Lösungen, die zwar Verschlüsselung anbieten, jedoch nur auf Basis von Software-Schlüsselpaaren, wesentlich erhöht. Die Gründe für die höhere Sicherheit sind: (1) Der private Schlüssel kann nie von Softwareanwendungen ausgelesen werden und (2) wird eine Zwei-Faktor-basierte Authentisierung („Besitz" der Karte und „Wissen" des PINs) bei der Entschlüsselung der Daten verwendet. Im Vergleich dazu verwenden bestehende Lösungen nur Passwörter für die Entschlüsselung von Daten, die direkt am Rechner des Benutzers gespeichert sind. Damit wird das Risiko erhöht, dass Passwörter mit Hilfe von Malware abgefangen werden können und somit unautorisierter Zugriff auf die verschlüsselten Daten ermöglicht wird.

Open Source Implementierung

Die CCE Software ist als Open Source veröffentlicht. Die Spezifikation vom verwendeten S/MIME Format ist ebenfalls öffentlich zugänglich. Dies ermöglicht somit eine einfache Erweiterbarkeit für spezifische Services. Somit können beispielsweise ganz einfach neue Cloud-Anbieter für das sichere Speichern integriert, neue Container-Formate verwendet oder andere Smart Cards inklusive neuer PKI-Infrastruktur hinzugefügt werden.

4.2.2 Nachteile

Dieser Abschnitt beschreibt die Nachteile unserer Lösung.

Web Interface und Mobile Version

Verglichen mit anderen Lösungen ist CCE derzeit nur in der Form von einer Desktop-Anwendung verfügbar. Es gibt zwar schon eine Parallelentwicklung für die Smartphone/Tablet-Plattformen iOS[13] und Android[14], dort steht man aber vor der Problematik des sicheren Aufbewahrens der verwendeten privaten Schlüssel. Hinsichtlich Benutzerfreundlichkeit und auch aufgrund der technischen Einschränkungen ist die Verwendung von Smart Cards auf mobilen Plattformen nicht oder nur mit sehr großen Umständen möglich. Ebenso gibt es im Moment noch keine Browser-Version, da man dort noch viel größere Probleme mit der sicheren Schlüsselaufbewahrung hat.

Keine Synchronisierung

Bestehende Cloud-Lösungen, welche ein sicheres und vertrauliches Speichern von Daten mittels Verschlüsselung anbieten, haben den Vorteil, dass die Daten automatisch und noch während dem Verschlüsselungsvorgang mit dem Cloud-Speicher synchronisiert werden. CCE bietet diese Möglichkeit jedoch nicht, da hier zuerst die Daten lokal verschlüsselt werden müssen, und erst danach ein Transfer zum Cloud-Speicher erfolgt.

Kartenleser

Die Verwendung von hardware-basierter Entschlüsselung mittels Smart Card setzt die Notwendigkeit zur Benutzung eines Kartenlesers voraus. Dies schränkt eventuell die Systemauswahl ein, da ein Kartenleser nicht immer zur Verfügung steht.

---

[13] Bereits verfügbar im Apple AppStore: SecureSend – https://itunes.apple.com/us/app/secure-send/id560086616?mt=8

[14] In den letzten Stufen der Entwicklung.

5 Umsetzung

In diesem Abschnitt wird genauer beschrieben, wie die Erweiterungen der CCE Software für eine Anbindung an diverse Public Cloud Provider umgesetzt wurden. Im ersten Teil wird erläutert, wie die CCE Software erweitert wurde, um einen einfachen und sicheren Datentransfer der CCE-verschlüsselten Container zu diversen Public Cloud Anbietern zu ermöglichen. Der zweite Teil beschäftigt sich mit der Einbindung von CCE und Cloud-Funktionalität in das Datei-System des gewählten Betriebssystems. Der letzte Teil zeigt Screenshots der adaptierten CCE Software, um den Mehrwert der Cloud-Funktionalität besser zu veranschaulichen.

5.1 Erweiterung der CCE Software

Beim Erweitern der CCE Software wurde gezielt Wert darauf gelegt, ein flexibles Hinzufügen weiterer Cloud Provider neben DropBox und Google Drive zu ermöglichen. Das Hinzufügen umfasst im Wesentlichen die Server-Kommunikation mit dem Cloud Provider sowie das Konfigurationsmanagement eines Cloud Providers, welches beides möglichst unabhängig implementiert werden kann. CCE ist dahingehend so modular implementiert und erweiterbar, dass neue Cloud Provider Konfigurationen ohne großen zusätzlichen Aufwand hinzugefügt werden können.

Die Erstellung einer Cloud Provider Konfiguration in CCE erfordert eine Smart Card, da somit eine personenbezogene Speicherung der Authentifizierungsinformationen[15] für den Cloud Provider Zugriff ermöglicht werden kann. Die Authentifizierungsinformationen werden dabei mit der Smart Card im lokalen Dateisystem verschlüsselt gespeichert und der jeweiligen Person zugeordnet. Es wird somit ein automatisches Mapping zwischen der Smart Card eines Benutzers und den cloud-spezifischen Authentifizierungsdaten, welche für einen Cloud Provider Zugriff notwendig sind, erreicht. Dies hat den Vorteil, dass die cloud-spezifischen Authentifizierungsdaten nur einmal eingegeben werden müssen und bei einem Cloud-Zugriff automatisch herangezogen werden können.

Im Detail sieht diese Konfiguration der Authentifizierungsinformationen für einen Cloud-Zugriff wie folgt aus. Die Authentifizierung zum Cloud Provider erfolgt sowohl bei DropBox als auch bei Google Drive mittels des Authentifizierungsprotokolls OAuth[16]. Die benötigten Authentifizierungstoken werden in einem ersten Schritt beim Hinzufügen eines Cloud Providers zu CCE ermittelt. Dies erfordert lediglich die Eingabe der Credentials des Benutzers, mit dessen Hilfe anschließend die Applikation CCE zum Cloud Provider als vertrauenswürdige Applikation hinzugefügt wird. Abschließend erhält CCE vom Cloud Provider ausgestellte Authentifizierungstoken für den sicheren Zugriff auf den Cloud Speicher. Gemäß dem OAuth Protokoll können diese Token laufend zur Cloud Provider Authentifizierung verwendet werden; daher ist weiters keine erneute Eingabe der Benutzer-Credentials notwendig.

Um Dateien in der Public Cloud zu speichern, kann ein Benutzer beim Verschlüsseln eine Speicheroption auswählen. Standardmäßig ist hierbei das lokale Dateisystem selektiert. Zusätzlich werden für diese Auswahl alle konfigurierten Cloud Provider angeboten, welche mit der aktiven Smart Card verknüpft sind. Beim Upload eines Containers werden die gespeicher-

[15] Derzeit werden nur Benutzername/Passwort Authentifizierungen unterstützt.

[16] http://oauth.net

ten Token des Cloud Providers mit der aktiven Smart Card entschlüsselt und zur Authentifizierung beim Cloud Provider verwendet.

5.2 Einbindung in das Datei-System

Um Benutzern eine vereinfachte Form des Uploads von Daten zu Public Cloud Providern anzubieten, ist es möglich, Dateien im Unterordner „CCE“ des benutzerspezifischen HOME-Verzeichnisses zu kopieren und anschließend mittels CCE-Verschlüsselungs-Wizard diese Dateien zu verschlüsseln. Nach der Verschlüsselung wird der Container zum entsprechenden Cloud Provider hochgeladen. Beim Erstellen neuer Dateien oder beim Verschieben von Dateien in das „CCE“-Verzeichnis wird der CCE-Verschlüsselungs-Wizard gestartet. Das Erkennen neu erstellter oder verschobener Dateien erfolgt mithilfe eines WatchServices[17], welches Dateisystemoperationen überwacht. Mithilfe dieses Wizards können nicht nur die Dateien automatisch verschlüsselt, sondern auch die Empfänger ausgewählt werden. Sollen die verschlüsselten Dateien an mehrere Benutzer verteilt werden, so kann dazu die vom Cloud Provider zur Verfügung gestellte Funktionalität verwendet werden.

5.3 Screenshots

In diesem Unterabschnitt werden ausgewählte Screenshots der adaptierten CCE-Software gezeigt, um die einzelnen Prozessschritte besser zu veranschaulichen. Es wird dabei in drei Prozesse unterschieden: Cloud Provider Konfiguration, Verschlüsselung, und Entschlüsselung.

5.3.1 Cloud Provider Konfiguration

Im Rahmen der Konfiguration kann ein Benutzer unterschiedliche Public Cloud Provider für ein Ablegen seiner CCE-Container-Daten in der CCE Software konfigurieren. Derzeit werden zwei der bekanntesten Public Cloud Provider für das Speichern von Daten in der Cloud unterstützt, nämlich DropBox und GoogleDrive. Abbildung 2 veranschaulicht diesen Konfigurationsprozess für den Public Cloud Anbieter DropBox.

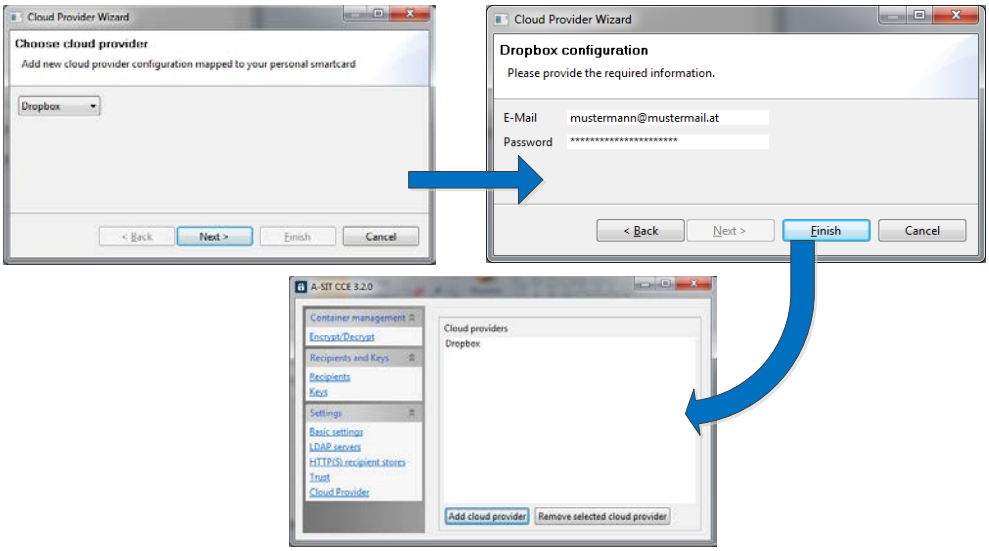

Abbildung 2 - Public Cloud Provider Konfiguration

[17] http://docs.oracle.com/javase/7/docs/api/java/nio/file/WatchService.html

5.3.2 Verschlüsselung

Der Verschlüsselungsprozess ist in Abbildung 3 gezeigt. Beim Verschlüsselungsprozess wählt der Benutzer in einem ersten Schritt jene Dateien aus, die er verschlüsselt in der Public Cloud ablegen möchte. Diese kann er entweder per Drag&Drop oder über einen File-System-Wizard auswählen. Anschließend kann er jene Benutzer auswählen, für die die Dateien verschlüsselt werden sollen. Nach Abbildung 3 will der Benutzer die Dateien nur für sich selbst verschlüsseln. Im nächsten Schritt wird der Benutzer um seinen PIN gefragt. Dies hat den Grund, dass die Credentials für den Zugriff auf den Cloud Speicher verschlüsselt abgelegt sind und daher zuerst entschlüsselt werden müssen. Für den eigentlichen Verschlüsselungsprozess wird der PIN jedoch nicht benötigt. Abschließend wählt der Benutzer noch einen Namen für den verschlüsselten CCE-Container, welcher danach im ausgewählten Cloud Speicher abgelegt wird.

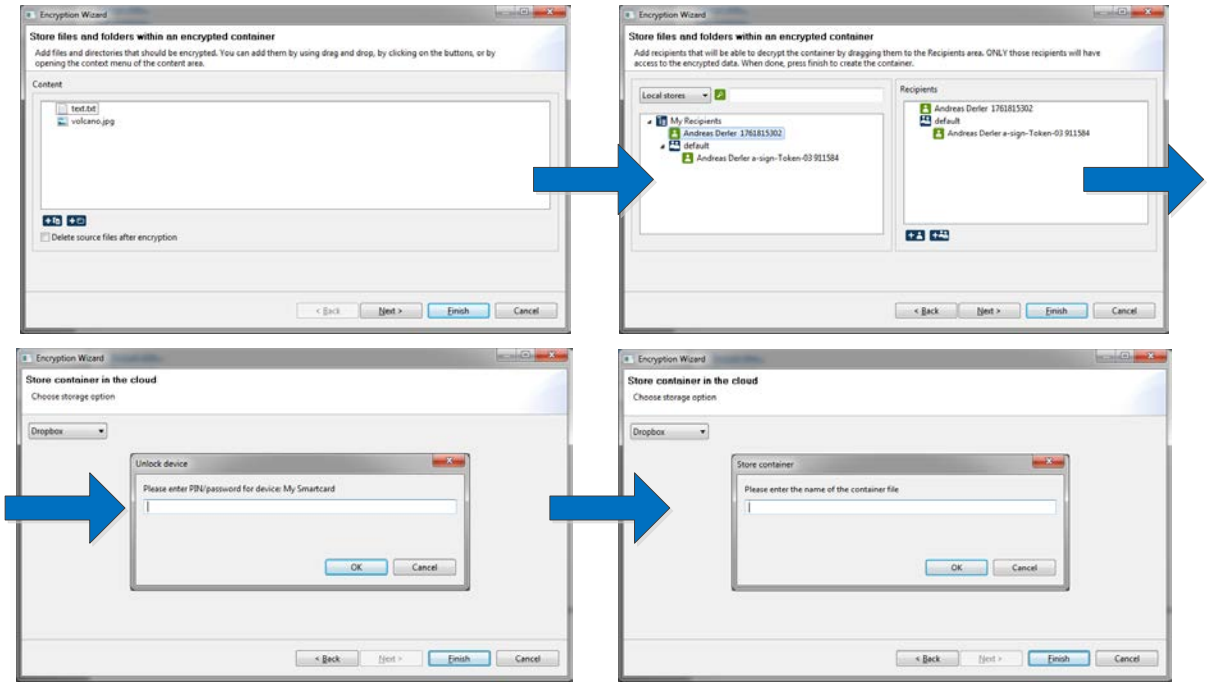

Abbildung 3 - Verschlüsselung mittels adaptierten CCE

5.3.3 Entschlüsselung

Beim Entschlüsselungsprozess wählt der Benutzer zuerst jenen CCE-Container aus der Cloud aus, den er entschlüsseln möchte. In dem in Abbildung 4 dargestellten Beispiel war der Container auf DropBox abgelegt. Im anschließenden Prozessschritt muss der Benutzer den entsprechenden Schlüssel zum Entschlüsseln auswählen. Im dargestellten Beispiel war die Bürgerkarte im Smart Card-Leser gesteckt und der Schlüssel wurde somit automatisch erkannt. Für das anschließende Entschlüsseln muss der Benutzer seinen PIN eingeben. Dieser Schritt ist hier nicht explizit dargestellt. Nach erfolgreicher Entschlüsselung muss der Benutzer nur noch das Verzeichnis am lokalen Rechner angeben, wohin die entschlüsselten Dateien abgelegt werden sollen. Danach stehen die entschlüsselten Dateien zur weiteren Verwendung im Klartext zur Verfügung.

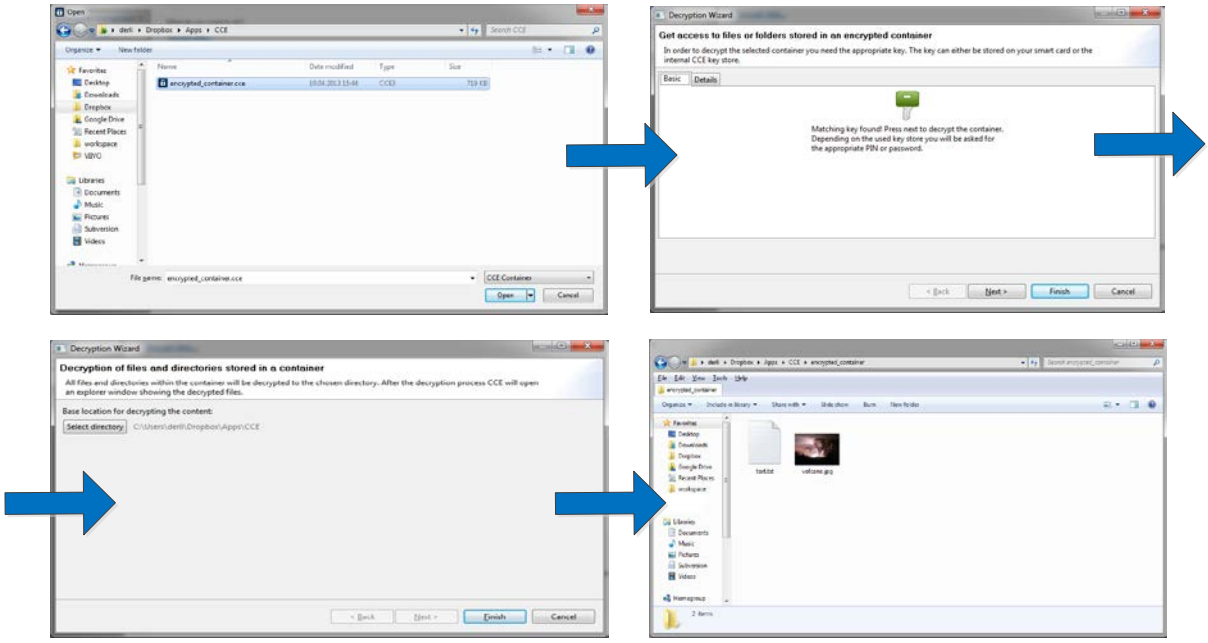

Abbildung 4 - Entschlüsselung mittels adaptierten CCE

6 Zusammenfassung und Ausblick

Das Speichern von Daten in der Public Cloud ist ein häufig angewandter Use Case. Um sensible Daten jedoch sicher und vertrauenswürdig in der Cloud abzuspeichern, sollten diese vor einem Transfer schon verschlüsselt worden sein. Es existieren bereits zahlreiche Lösungen, die ein client-seitiges Verschlüsseln ermöglichen. Diese Lösungen haben jedoch den Nachteil, dass das Schlüsselpaar zum Ver- und Entschlüsseln von Daten nur software-mäßig gespeichert wird. Im Gegensatz dazu setzt unsere vorgestellte Lösung mittels CCE auf Schlüsselpaare, die hardwaremäßig gesichert sind, und somit wird ein höheres Sicherheitsniveau erreicht. Wir haben dabei CCE so erweitert, dass Daten mit Bürgerkarten verschlüsselt auf unterschiedlichen Public Cloud Provider Plattformen abgelegt werden können. Benutzer sind damit auch nicht mehr von einem bestimmten Public Cloud Provider abhängig.

Es gibt mehrere Richtungen, in welche die Funktionalitäten und Features von CCE weiter entwickelt werden könnten. Es ist geplant, die Versionen für den Desktop, sowiedie sich gerade in Parallelentwicklung befindlichen Versionen für iOS und Android zu vereinheitlichen, die Problematik der sicheren Schlüsselaufbewahrung auf diesen Plattformen zu lösen, und auch Überlegungen in Richtung einer sicheren Browser-Version anzustellen. Eine weitere Erweiterung könnte sein, Daten nicht nur bei einem Cloud Provider abzulegen sondern redundant auf mehreren Providern zu verteilen. Letztendlich wäre es noch eine praktikable Möglichkeit, die CCE-Container im Dateisystem zu mounten und somit die Sichtbarkeit von verschlüsselten Dateien im Dateisystem zu ermöglichen.

Literatur

[DHC+12] M. H. Diallo, B. Hore, E. Chang, S. Mehrotra, N. Venkatasubramanian: CloudProtect: Managing Data Privacy in Cloud Applications, In IEEE CLOUD, S. 303–310, 2012

[DropBox] DropBox: Where does dropbox store everyone's data? 2013, https://www.dropbox.com/help/7/en

[EGovG] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz - E-GovG) StF: BGBl. I Nr. 10/2004

[EP95] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23/11/1995 S. 0031 – 0050

[HKR+08] A. Hollosi, G. Karlinger, T. Rössler, M. Centner: Die österreichische Bürgerkarte, Version 1.2, 2008, http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/

[LHP02] H. Leitold, A. Hollosi, R. Posch: Security Architecture of the Austrian Citizen Card Concept, 18th Annual Computer Security Applications Conference (ACSAC), 2002

[RT04] B. Ramsdell, S. Turner (2004): Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC 3851, 2004, http://www.ietf.org/rfc/rfc3851.txt

[SGS11] R. Seiger, S. Gross, A. Schill: SECCSIE: A secure cloud storage integrator for enterprises, In IEEE 13th Conference on Commerce and Enterprise Computing (CEC), S. 252–255, 2011

[SigR] RICHTLINIE 1999/93/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen